業　務　仕　様　書

1　委託業務名

役務番号　第21556号

市立札幌病院外部ネットワークセキュリティ脆弱性診断業務

2　業務概要

平成28年４月１日付で札幌市総務局情報システム部より通知された「札幌市情報セキュリティ技術対策基準」に基づき、外部に公開するサーバーおよび境界ネットワーク機器に対して、年１回以上のセキュリティ脆弱性診断の実施が義務付けられている。

市立札幌病院（以下、「委託者」という。）の情報システム担当係の運用管理している範囲においては、「総合医療情報システムのリモートメンテナンス用ネットワーク機器」および「感染症臨床研究事業用ネットワーク機器」の２機器（２系統）が該当する。そのため、これら外部から参照可能となるネットワーク機器に対してセキュリティ脆弱性診断を行い、セキュリティ対策状況を専門的な視点から確認し、今後のセキュリティ対策の強化を図ることを目的とする。

3　履行期間

契約締結日から令和９年３月１２日（金）まで

4　履行場所

札幌市中央区北11条西13丁目１－１　市立札幌病院

※診断作業は、受託者の事業所等から遠隔で実施して差し支えない。

5　業務内容

(1) セキュリティ脆弱性診断

ア　診断対象

本業務の診断対象は、総合医療情報システムのリモートメンテナンス用ネットワーク機器、ならびに、感染症臨床研究事業用ネットワーク機器であり、それぞれ1つのグローバルIPアドレスを持つことから2つのIPアドレスを対象とする。なお、対象IPアドレス等の接続情報は、契約締結後に委託者が受託者へ提示する。

上記の診断対象機器に対して、下記の診断を行うこと。

・ポートスキャン（オープンされているポートを検出する）

・脆弱性スキャン(既知の脆弱性有無を検出する)

イ　作業計画および事前調整

受託者は、診断作業前に診断内容やデータ収集期間、診断方法、診断日時、シス

テム運用への影響等について、委託者と作業計画の協議・調整を行い、事前に承諾を得ること。

ウ 安全への配慮

病院業務および通信環境に影響を及ぼさないよう配慮し、大量のトラフィックを発生させる過度な負荷テスト（DoS 攻撃等）や、機器停止・再起動を招くおそれのあるスキャンは除外すること。

(2) 診断結果報告

診断結果について、報告書を日本語で作成し、提出すること。また、報告書の書式については、事前に委託者に提案を行い、承諾を得ること。

具体的な報告内容は以下の通りとする。

ア　診断実施日

イ　診断項目

ウ　診断対象機器毎の診断結果（セキュリティリスクの解説や想定される影響）

エ　診断結果からの考察（検出された脆弱性の推奨される対策）

6　納品物

診断結果報告書

7　一般・共通事項

(1) 外部に公開しているネットワーク機器は 24 時間 365 日運用しており、診断する日時や手順等について、事前に委託者に説明をし、必ず承諾を得た上で実施すること。

(2) 診断作業後にシステム障害が発生した場合には、診断前の状態にサーバーを復旧させるよう協力すること。

(3) 本仕様書に明記されていない事項については、当院と受託者が誠意をもって協議し、決定するものとする。

(4) 業務従事者は、業務上知り得た情報を他に漏らさず、発注者の許可なく本業務以外の目的のために使用してはならない。

(5) 疑義等の解消

契約書および当仕様書における疑義、又は業務を遂行する上での疑義が生じた場合は、その都度受託者は委託者へ内容の確認を行い疑義の解消を行うこと。

また、仕様書において定めのない事項で業務遂行上定める必要のある事項が生じた際には、その都度、受託者と委託者が協議の上定めることとする。